

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION  
International Bureau



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : <b>G06F 1/00, 12/14</b>	A1	(11) International Publication Number: <b>WO 95/14266</b> (43) International Publication Date: <b>26 May 1995 (26.05.95)</b>
(21) International Application Number: <b>PCT/US94/12457</b>		(81) Designated States: AU, CA, JP, KR, NO, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).
(22) International Filing Date: <b>28 October 1994 (28.10.94)</b>		Published <i>With international search report.</i>
(30) Priority Data: 152,804 15 November 1993 (15.11.93) US		
(71) Applicant: HUGHES AIRCRAFT COMPANY [US/US]; 7200 Hughes Terrace, Los Angeles, CA 90045 (US).		
(72) Inventors: HAYES, John, L.; 175 B North Magnolia, Anaheim, CA 92801 (US). HYMAN, Paul, M.; 811 Azalea Avenue, Placentia, CA 92670 (US).		
(74) Agents: WALDER, Jeannette, M. et al; Hughes Aircraft Company, Building C1, M/S A126, P.O. Box 80028, Los Angeles, CA 90080-0028 (US).		
(54) Title: A METHOD AND SYSTEM FOR MAINTAINING ACCESS SECURITY OF INPUT AND OUTPUT OPERATIONS IN A COMPUTER SYSTEM		
(57) Abstract		
Disclosed is a computer system and a method under which a personal computer or a workstation may use commercial off-the-shelf software application packages with a commercially available operating system while providing features of multi-level security including mandatory access controls and propagation of classification levels and codewords when information is moved between documents. Users are allowed to manually reclassify documents (including downgrading) as necessary. The present invention may also be embodied to provide security when computer are on a network by means of a secure file server.		

***FOR THE PURPOSES OF INFORMATION ONLY***

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	GB	United Kingdom	MR	Mauritania
AU	Australia	GE	Georgia	MW	Malawi
BB	Barbados	GN	Guinea	NE	Niger
BE	Belgium	GR	Greece	NL	Netherlands
BF	Burkina Faso	HU	Hungary	NO	Norway
BG	Bulgaria	IE	Ireland	NZ	New Zealand
BJ	Benin	IT	Italy	PL	Poland
BR	Brazil	JP	Japan	PT	Portugal
BY	Belarus	KE	Kenya	RO	Romania
CA	Canada	KG	Kyrgyzstan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo	KR	Republic of Korea	SE	Sweden
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LJ	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LU	Luxembourg	TD	Chad
CS	Czechoslovakia	LV	Latvia	TG	Togo
CZ	Czech Republic	MC	Monaco	TJ	Tajikistan
DE	Germany	MD	Republic of Moldova	TT	Trinidad and Tobago
DK	Denmark	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	US	United States of America
FI	Finland	MN	Mongolia	UZ	Uzbekistan
FR	France			VN	Viet Nam
GA	Gabon				

1                   **A METHOD AND SYSTEM FOR**  
2                   **MAINTAINING ACCESS SECURITY OF INPUT AND OUTPUT**  
3                   **OPERATIONS IN A COMPUTER SYSTEM**

4                   **BACKGROUND OF THE INVENTION**

5                   1. Field of the Invention

6                   This invention relates in general to computer security  
7                   systems, and, more particularly, to a computer security  
8                   system and a method for automatically limiting user access  
9                   to information stored in the computer in accordance with a  
10                  predetermined, but variable, user security profile of  
11                  permissible operations for each user that aids the user in  
12                  properly classifying documents.

13                  2. Description of the Related Art

14                  Previous implementations of secure computer  
15                  workstations required the use of a special operating system  
16                  and could not provide security when commercial off-the-  
17                  shelf ("COTS") software application packages were used.  
18                  Such systems, commonly called "Compartmented Workstations",  
19                  are notoriously inconvenient to use and do not allow for  
20                  data merger of documents and downgrading of documents.

21                  In general, these previous implementations do not: (1)  
22                  run on the popular, commercially available computers; (2)  
23                  allow usage of a broad spectrum of COTS applications and  
24                  not just "trusted" applications that have been security  
25                  tested or qualified; (3) allow merger of data of different  
26                  security levels; (4) allow usage of the standard operating  
27                  system.

28                  **OBJECTS AND SUMMARY OF THE INVENTION**

29                  Therefore, it is an object of the present invention to  
30                  provide a method and system for providing security for  
31                  documents and data that does not require the use of  
32                  "trusted" applications only, but allows usage of commercial  
33                  off-the-shelf software application packages.

34                  It is still another object of the present invention to

1 provide a method and system for providing security for  
2 documents and data that provides propagation of security  
3 labels when data is moved between documents.

4 It is still another object of the present invention to  
5 provide a method and system for providing security for  
6 documents and data that puts the users in control of their  
7 documents provided that they have necessary security access  
8 rights.

9 It is another object of the present invention to  
10 provide a method and system for providing security for  
11 documents and data that facilitates, rather than prevents,  
12 data merger of documents classified at different security  
13 levels.

14 It is yet another object of the present invention to  
15 provide a method and system for providing security for  
16 documents and data that not only prevents unauthorized  
17 access to files and data, but which also aids the user in  
18 properly classifying documents and data retained on the  
19 system or manipulated by the method of the present  
20 invention.

21 Other objects of the present invention are: it does  
22 not require the development of a "trusted" operating  
23 system, but rather exists as an extension to the existing  
24 operating system; provides security of documents on a  
25 network at the workstation level; concentrates on  
26 "detection and audit" of "curious," "hostile" or  
27 "mischievous" action by users as opposed to "prevention" of  
28 such so that more trust is placed on the users allowing for  
29 a more user friendly system.

30 The present invention provides a computer system and  
31 a method under which a personal computer or a workstation  
32 may use commercial off-the-shelf software application  
33 packages with a commercially available operating system  
34 while providing features of multi-level security including  
35 mandatory access controls and propagation of classification  
36 levels and codewords when information is moved between  
37 documents. Users are allowed to manually reclassify

1 documents (including downgrading subject to restrictions)  
2 as necessary. The present invention may also be embodied  
3 to provide security when computer are on a network by means  
4 of a secure file server.

5 The novel features of construction and operation of  
6 the invention will be more clearly apparent during the  
7 course of the following description, reference being had to  
8 the accompanying drawings wherein has been illustrated a  
9 preferred form of the device of the invention and wherein  
10 like characters of reference designate like parts  
11 throughout the drawings.

12 **BRIEF DESCRIPTION OF THE FIGURES**

13 FIGURE 1 is a block diagram flowchart showing the  
14 general overall logic flow through a system incorporating  
15 the present invention;

16 FIGURE 2 is an idealized block diagram flowchart  
17 showing the general overall operational flow through a  
18 system incorporating the present invention;

19 FIGURE 3 is an idealized diagram showing the various  
20 input/output operations occurring in a system embodying the  
21 present invention; and,

22 FIGURE 4 is an idealized block diagram showing a  
23 structure for the User Access Table and acceptable sub-  
24 field structure.

25 **DESCRIPTION OF THE PREFERRED EMBODIMENT**

26 A preferred form of the invention as embodied in a  
27 method and computing system for providing occurrence level,  
28 value based security protection, limiting for each user  
29 access to preselected, but variable Input/Output operations  
30 on selected data objects in the computer system is now  
31 described.

32 In general, as shown in FIGURE 1, the invention is  
33 found in a computer system interfacing Input/Output  
34 requests between at least one user, identified by a unique  
35 user identification symbol, and the computer system having

1 at least one data object containing data therein. The  
2 method comprises operating the computer to automatically  
3 perform the following steps.

4 A data object security access label, representing a  
5 security profile defining a user security access level and  
6 the Input/Output operations permitted on the data object,  
7 is established and associated with each data object  
8 selected for security protection 10. Such data objects are  
9 always given this security access label and include "saved"  
10 documents or text files generated by the application  
11 programs that may be running on the computer system.

12 A user security access table is also established 12  
13 that has, for each user selected to have Input/Output  
14 access to the data objects in the computer system, a first  
15 entry identifying the user by the unique user  
16 identification symbol, and a second entry representing a  
17 user security profile for the particular user. The second  
18 entry is used to define the security access level of the  
19 associated user.

20 A session security level "flag" is set to a  
21 preselected default condition representing one of the  
22 security access levels 14.

23 Each user request to the computer system is parsed to  
24 extract each Input/Output request 16. For each of the  
25 found Input/Output requests (1) the unique user  
26 identification symbol of the user making the Input/Output  
27 request; (2) the data object that is the subject of the  
28 Input/Output request; and (3) the requested Input/Output  
29 operation are then extracted.

30 The unique user identification symbol is compared with  
31 the first entry of the user security access table. a user  
32 security access "flag" at the computer system is set to an  
33 "allowed" condition and a user security level "flag" is set  
34 to the security access level defined by the second entry of  
35 the user security access table associated with the user  
36 identification symbol if a match is found, and otherwise  
37 setting each "flag" to a "denied" condition 18.

1       The requested Input/Output operation being requested  
2       is compared with the data object security access label  
3       associated with the data object that is the subject of the  
4       Input/Output request, and at the computer system a data  
5       object security access "flag" is set to an "allowed"  
6       condition if a match is found and otherwise to a "denied"  
7       condition 20.

8       The session security level "flag" is compared to the  
9       user security access level defined in the security profile  
10      for the data object that is the subject of the Input/Output  
11      request, and the session security level "flag" is set to  
12      the predetermined "higher" security level 22.

13      Once the flags have been set, the Input/Output request  
14      is returned to the computer system for processing whenever  
15      the user security access "flag" and the data object  
16      security access "flag" are both in the "allowed" condition  
17      24.

18      It is also preferred that the method of the present  
19      invention including writing at the computer system to a  
20      security violation log the unique user identification  
21      symbol whenever the user security access flag, the user  
22      security level flag or the data object security access flag  
23      is in said "denied" condition, and canceling the execution  
24      of the parsed Input/Output request by the computer system.

25      Similarly, it is also preferred that when a violation  
26      or attempted breach of security is discovered, the  
27      invention returns a preselected message to the computer  
28      system user whenever the user security access flag, the user  
29      security level flag or the data object security access  
30      flag is in the "denied" condition.

31      Also, for ease of changing the various security levels  
32      on the various data objects held in the computer system, it  
33      is preferred that the method allow the computer system user  
34      to access and modify the data object security label  
35      whenever the user security access flag, the user security  
36      level flag, and the data object security access flag are  
37      each in an "allowed" condition.

1        Finally, the data object security access label, the  
2        user security access table and session security level flags  
3        are preferably retained at the computer system until the  
4        computer system user logs off the computer system.

5        In Figure 2, the present invention is shown in an  
6        idealized block diagram flowchart showing the general  
7        overall operational flow through a system incorporating the  
8        present invention where a user 26 has launched two  
9        applications 28, 30, respectively. As shown in the  
10      drawing, the user 26 and each application 28, 30, has a  
11      Security Label 26a, 28a, 30a respectively, associated with  
12      it. The Security Labels are a data structure which defines  
13      access requirements, and propagation restrictions for data  
14      and/or files retained on the system. Examples of such  
15      Security Labels include hierarchial classifications such as  
16      Confidential, Secret, Top Secret and/or a series of  
17      categories or "Tickets" such as various assigned  
18      "codewords".

19      Whenever an application requests an input/output  
20      operation on a document, such as a application 28  
21      requesting to read a document 32, the document labels (here  
22      shown as 32a) associated with the requested documents are  
23      added to the application's label 28a. The application 28  
24      cannot open any document to which the user 26 does not have  
25      access as determined by the user label 26a associated with  
26      the user at logon and user identification.

27      When an application label increases, the session label  
28      34, displayed on the screen for the user, is also  
29      increased.

30      Conversely, when an application such as 30 writes a  
31      document (here shown as 36), any additional categories are  
32      noted and written into the document's label 36a. If the  
33      security level of the application as then running is higher  
34      than the document's original security level, the higher  
35      security level is noted. The user can see what the new  
36      label is and either accept it or change it as described  
37      below.

1        In Figures 3 and 4, the present invention is shown in  
2        an idealized diagram showing the various input/output  
3        operations occurring in a system embodying the present  
4        invention. A user 40 generates an operator request 42 to  
5        the operating system 44 to launch one or more system  
6        included applications 46 resulting in an executing  
7        "Instance" of those programs, for input/output operation on  
8        files 54 available on the system. The applications  
9        programs in turn make the necessary input/output requests  
10      50 and 52 to read and write the user requested files.

11       There exists a Clipboard 55 which implements a  
12       temporary holding buffer for data that is to be copied and  
13       pasted between files. These read and write operations 56  
14       and 57 are performed by the application instance per user  
15       request.

16       In addition there is a means for the user 40 to  
17       request that a user-selected portion of the screen 66 by  
18       read 59 into the Clipboard 55 for subsequent pasting of  
19       that image into any file 54. Each file, the Clipboard,  
20       each Application Instance and the Screen has a Security  
21       Label 58 associated with it as shown in Figure 3 containing  
22       various fields of information. The Security Label 58  
23       associated with of these objects 46, 54, 55 and 59, may  
24       contain several fields, such as a Classification Level, any  
25       required access "Tickets", and a Restrictions format such  
26       as "no copy", "no print", "no export", or "originator only  
27       downgrade". Likewise, a User Access Table 60 is  
28       established for verification of the user's identity and  
29       access profile and includes such fields 62 as: "user  
30       identification", "user password", "user level access",  
31       "user tickets map". At logon, the User Access Table 60 is  
32       accessed by the system to determine and establish the  
33       identity and classification access profile of the  
34       individual user 40 requesting to login to the system 65.

35       While the above description emphasizes the method and  
36       system of the present invention in comparing user access  
37       levels with document access levels and disallowing access

1       when the user access does not match, there are other  
2       important novel and non-obvious aspects of the present  
3       invention described below.

4           One such additional important design consideration,  
5       based on the needs of the users for which the system is  
6       intended, is the capability to merge documents of different  
7       classifications while aiding the user in determining the  
8       proper classification for the resulting document.

9           For example, a user may wish to make a presentation  
10      describing a plan that he is working on, and may copy text  
11      and pictures from other documents having security labels of  
12      different security levels to create a composite  
13      presentation document in the course of making the  
14      presentation. The system and method of the present  
15      invention "observes" or intercepts all data which enters  
16      the application being used to prepare the presentation  
17      document, and determines a classification for all documents  
18      written by the application based upon a preselected  
19      weighing of all of the individual classifications found in  
20      each separate document or piece of data being assembled  
21      into the final presentation. Upon user request the  
22      invention then offers its suggested classification for the  
23      composite presentation document to the user.

24           If the user does nothing to reclassify the document,  
25      the present invention automatically assigns the document  
26      its suggested classification. The invention also  
27      distinguishes for the user the original classification of  
28      each document and the labels which it believes may have  
29      been included in creating the composite presentation  
30      document (via various cut and paste, and other I/O  
31      operations such as reading a file).

32           The user is given the capability to accept the  
33      suggested classification label or to downgrade or upgrade  
34      the document as he sees fit. This is in contrast to  
35      compartmented-mode workstations which require the user to  
36      log in at a particular security level and not create any  
37      documents classified at any lower level nor access

1 documents classified at a higher level, making such  
2 workstations unsuitable for the task outlined above.

3 By treating applications as a "black box" and  
4 observing all data going in and out of the applications,  
5 the present invention allows the use of commercial-off-the  
6 -shelf applications and does not require any special  
7 security features in the applications software being run on  
8 a system embodying the present invention, i.e., "trusted"  
9 or "certified" software.

10 The actions of the invention are at times more complex  
11 than that outlined above. For example, not only is the  
12 classification level of each application maintained and  
13 assigned to documents written by that particular  
14 application, but the classification level of the entire  
15 session is maintained as well. Therefore, if the user  
16 takes a screen snapshot and pastes it in a document, the  
17 entire session label is applied to that document, since  
18 portions of the screen owned by any other concurrently  
19 running applications displaying data, may have been  
20 included in the screen snapshot.

21 The further operation of a method and system embodying  
22 the present invention is now described using the following  
23 terms:

24 Application Instance - an application currently  
25 executing on the system;

26 Security Label - a data structure which defines access  
27 requirements, and propagation restrictions for data and/or  
28 files retained on the system. Examples of such Security  
29 Labels include hierachial classifications such as  
30 Confidential, Secret, Top Secret and/or a series of  
31 categories or "Tickets" such as various assigned  
32 "codewords".

33 Tickets - additional Security Labels restricting a  
34 file or data to a select group granted a "ticket" for  
35 access.

36 Clipboard - the operating system's inter-application  
37 cut/copy/paste buffer utility;

1       Maximize - the combining of two security labels in  
2       accord with a pre-determined algorithm such as a selected  
3       set of weighted selection values.

4       The method and system of the present invention runs  
5       concurrently with the operating system to intercept any  
6       Input/output service calls to the operating system as  
7       follows:

8       1. Whenever the operating system "launches" an  
9       application (an Application Instance), this interception  
10      entails the following steps:

11      A. The Security Label of the Application Instance is  
12      set to the preselected Startup Application Security Label;

13      B. If the Security Label indicates that the Clipboard  
14      buffer contains data which cannot be downgraded in  
15      classification, it prompts the user to either allow the  
16      read (and thus Maximize the Security Label of the  
17      Application Instance with that of the Clipboard) or to  
18      delete the contents of the Clipboard buffer, leaving the  
19      Security Label of the Application Instance as it originally  
20      was.

21      C. If the Application Instance performs an automatic  
22      read of the Clipboard buffer, and the Security Label  
23      indicates that the data does not contain data which cannot  
24      be downgraded, then Maximize the Security Label of the  
25      Application Instance with that of the Clipboard buffer.

26      D. Recalculate the Security Label of the screen as a  
27      Maximization of the Security Labels of all Application  
28      Instances.

29      2. Whenever an Application Instance performs an open  
30      of a file, this interception entails the following steps:

31      A. Maximize the Security Label of the Application  
32      Instance with the Security Label of the file being opened.

33      B. Recalculate the Security Label of the screen as a  
34      Maximization of the Security Labels of all Application  
35      Instances.

36      3. Whenever an Application Instance performs a write  
37      to a file, this interception entails the following steps:

- 1        A. Set the Security Label of the file to the Security  
2        Label of the Application Instance.
- 3        B. Do not allow any write if there is a "no copy"  
4        restriction on the data or file.
- 5        4. Whenever an Application Instance terminates, this  
6        interception entails the following steps:
  - 7            A. Recalculate the Security Label of the screen as a  
8            Maximization of the Security Labels of all the remaining  
9            Application Instances.
  - 10          5. Whenever an attempt is made to "boot" or start-up  
11          the operating system of the computer in the system, this  
12          interception entails the following steps:
    - 13            A. Prompt the user for username/password.
    - 14            B. If username/password does not exist in the User  
15            Access Table, then shutdown and deny any further access to  
16            the system.
    - 17            C. Otherwise, if the username/password is found in  
18            the User Access Table, then set the Security Label of the  
19            screen to the preselected Startup Screen Security Label.
  - 20          6. Whenever an Application Instance performs a read  
21          from the Clipboard, this interception entails the following  
22          steps:
    - 23            A. Maximize the Security Label of the Application  
24            Instance with the Security Label of the Clipboard.
    - 25            B. Recalculate the Security Label of the screen as a  
26            Maximization of the Security Labels of all Application  
27            Instances.
  - 28          7. Whenever an Application Instance performs a write  
29          to the Clipboard, this interception entails the following  
30          steps:
    - 31            A. Set the Security Label of the Clipboard to the  
32            Security Label of the Application Instance.
    - 33            8. Whenever an Application Instance performs a print  
34            of a file, this interception entails the following steps:
      - 35            A. Do not allow the print if a "no print" restriction  
36            on the data or file.
      - 37            B. Stamp the Security Label on all pages.

1       The following Utilities embody features found in the  
2       present invention:

3       A first Utility provides a means to display and allow  
4       the user to modify, with restrictions, the Security Label  
5       of a file as follows:

6           A. Upon user request, the utility displays the  
7       Security Label of the selected file;

8           B. The utility also provides a means to differentiate  
9       for the user the Security Level and Tickets applied by the  
10      security software from the Security Level and Tickets  
11      applied by the user to the file.

12          C. The utility prohibits certain Security Label  
13      changes based on user-tailorable Restrictions.

14          A second Utility, upon user request, provides a means  
15      to display the Security Label of a selected Application  
16      Instance.

17          A third Utility provides a means to display the  
18       Security Label of the screen by making it always visible  
19       during a user session. Thus, constantly reminding the user  
20       of the various classification levels of documents appearing  
21       on the screen.

22          A fourth Utility provides a means for the user to  
23      select a portion of the screen and take a "picture" of it,  
24      putting the results into the Clipboard buffer for later  
25      manipulation by the user.

26          A fifth Utility provides a means for the operator to  
27      define the User Access Table, the Security Levels and  
28      "Tickets", the Startup Screen Security label, and the  
29      Startup Application Security Label.

30          The invention described above is, of course,  
31      susceptible to many variations, modifications and changes,  
32      all of which are within the skill of the art. It should be  
33      understood that all such variations, modifications and  
34      changes are within the spirit and scope of the invention  
35      and of the appended claims. Similarly, it will be  
36      understood that Applicant intends to cover and claim all  
37      changes, modifications and variations of the example of the

1 preferred embodiment of the invention herein disclosed for  
2 the purpose of illustration which do not constitute  
3 departures from the spirit and scope of the present  
4 invention.

## WHAT IS CLAIMED IS:

1. In a computer system interfacing Input/Output requests between at least one user, identified by a unique user identification symbol, and the computer system having at least one data object containing data therein, a method for providing occurrence level, value based security protection, limiting for each user access to preselected, but variable Input/Output operations on selected data objects in the computer system, said method comprising operating the computer to automatically perform the steps of:
  11. establishing and associating with each data object selected for security protection, a data object security access label representing a security profile defining a user security access level and the Input/Output operations permitted on the data object;
  16. establishing a user security access table having, for each user selected to have Input/Output access to the data objects in the computer system, a first entry identifying the user by the unique user identification symbol, and a second entry representing a user security profile associated therewith, said second entry defining the security access level of the associated user;
  23. set a session security level "flag" to a preselected default condition representing one of said security access levels;
  26. parsing each Input/Output request from the user to the computer system and extracting therefrom (1) the unique user identification symbol of the user making the Input/Output request; (2) the data object that is the subject of the Input/Output request; and (3) the requested Input/Output operation;
  32. comparing the unique user identification symbol with the first entry of the user security access table and setting at the computer system a user security access "flag" to an "allowed" condition and a user security level "flag" to the security access level defined by the second

37 entry of the user security access table associated with the  
38 user identification symbol if a match is found, and  
39 otherwise setting each "flag" to a "denied" condition;

40 comparing the requested Input/Output operation being  
41 requested with the data object security access label  
42 associated with the data object that is the subject of the  
43 Input/Output request, and setting at the computer system a  
44 data object security access "flag" to an "allowed"  
45 condition if a match is found and otherwise to a "denied"  
46 condition;

47 comparing the session security level "flag" to the  
48 user security access level defined in the security profile  
49 for the data object that is the subject of the Input/Output  
50 request, and setting the session security level "flag" to  
51 the predetermined "higher" security level;

52 returning the Input/Output request to the computer  
53 system for processing whenever said user security access  
54 "flag" and said data object security access "flag" are both  
55 in said "allowed" condition.

1           2. A method as in claim 1, further including the  
2 steps of:

3           writing at the computer system to a security violation  
4 log the unique user identification symbol whenever said  
5 user security access flag, said user security level flag or  
6 said data object security access flag is in said "denied"  
7 condition and canceling the execution of the parsed  
8 Input/Output request by the computer system.

1           2. A method as in claim 1, further including the  
2 steps of:

3           returning a preselected message to the computer system  
4 user whenever said user security access flag, said user  
5 security level flag or said data object security access  
6 flag is in said "denied" condition and canceling the  
7 execution of the parsed Input/Output request by the  
8 computer system.

1           4. A method as in claim 1, further including the  
2           steps of:

3           allowing the computer system user to access and modify  
4           the data object security label whenever said user security  
5           access flag, said user security level flag, and said data  
6           object security access flag are each in said "allowed"  
7           condition.

1           5. A method as in claim 1, further including the  
2           steps of:

3           retaining said data object security access label, said  
4           user security access table and said session security level  
5           flag until the computer system user logs off the computer  
6           system.

1           6. In a computer system interfacing Input/Output  
2           requests between at least one user, identified by a unique  
3           user identification symbol, and the computer system having  
4           at least one data object containing data therein, a method  
5           for providing occurrence level, value based security  
6           protection, limiting for each user access to preselected,  
7           but variable Input/Output operations on selected data  
8           objects in the computer system, said method comprising  
9           operating the computer to automatically perform the steps  
10          of:

11          establishing and associating with each data object  
12          selected for security protection, a data object security  
13          access label representing a security profile defining a  
14          user security access level and the Input/Output operations  
15          permitted on the data object;

16          establishing a user security access table having, for  
17          each user selected to have Input/Output access to the data  
18          objects in the computer system, a first entry identifying  
19          the user by the unique user identification symbol, and a  
20          second entry representing a user security profile  
21          associated therewith, said second entry defining the  
22          security access level of the associated user;

23           set a session security level "flag" to a preselected  
24        default condition representing one of said security access  
25        levels;

26           parsing each Input/Output request from the user to the  
27        computer system and extracting therefrom (1) the unique  
28        user identification symbol of the user making the  
29        Input/Output request; (2) the data object that is the  
30        subject of the Input/Output request; and (3) the requested  
31        Input/Output operation;

32           comparing the unique user identification symbol with  
33        the first entry of the user security access table and  
34        setting at the computer system a user security access  
35        "flag" to an "allowed" condition and a user security level  
36        "flag" to the security access level defined by the second  
37        entry of the user security access table associated with the  
38        user identification symbol if a match is found, and  
39        otherwise setting each "flag" to a "denied" condition;

40           comparing the requested Input/Output operation being  
41        requested with the data object security access label  
42        associated with the data object that is the subject of the  
43        Input/Output request, and setting at the computer system a  
44        data object security access "flag" to an "allowed"  
45        condition if a match is found and otherwise to a "denied"  
46        condition;

47           comparing the session security level "flag" to the  
48        user security access level defined in the security profile  
49        for the data object that is the subject of the Input/Output  
50        request, and setting the session security level "flag" to  
51        the predetermined "higher" security level;

52           returning the Input/Output request to the computer  
53        system for processing whenever said user security access  
54        "flag" and said data object security access "flag" are both  
55        in said "allowed" condition;

56           writing at the computer system to a security violation  
57        log the unique user identification symbol whenever said  
58        user security access flag, said user security level flag or  
59        said data object security access flag is in said "denied"

60 condition and canceling the execution of the parsed  
61 Input/Output request by the computer system;  
62 returning a preselected message to the computer system  
63 user whenever said user security access flag, said user  
64 security level flag or said data object security access  
65 flag is in said "denied" condition and canceling the  
66 execution of the parsed Input/Output request by the  
67 computer system;  
68 allowing the computer system user to access and modify  
69 the data object security label whenever said user security  
70 access flag, said user security level flag, and said data  
71 object security access flag are each in said "allowed"  
72 condition;  
73 retaining said data object security access label, said  
74 user security access table and said session security level  
75 flag until the computer system user logs off the computer  
76 system.

1/4

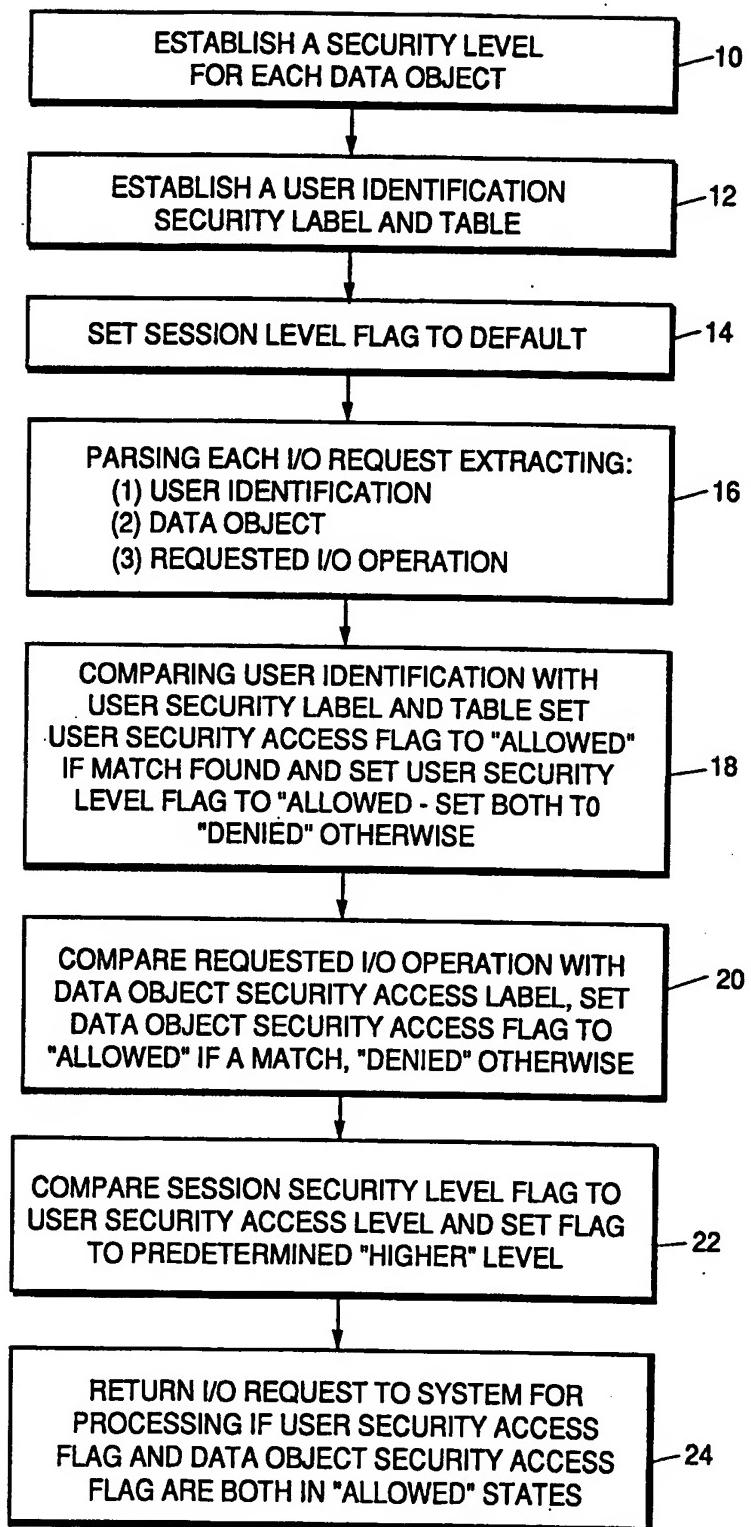


FIG. 1.

2/4

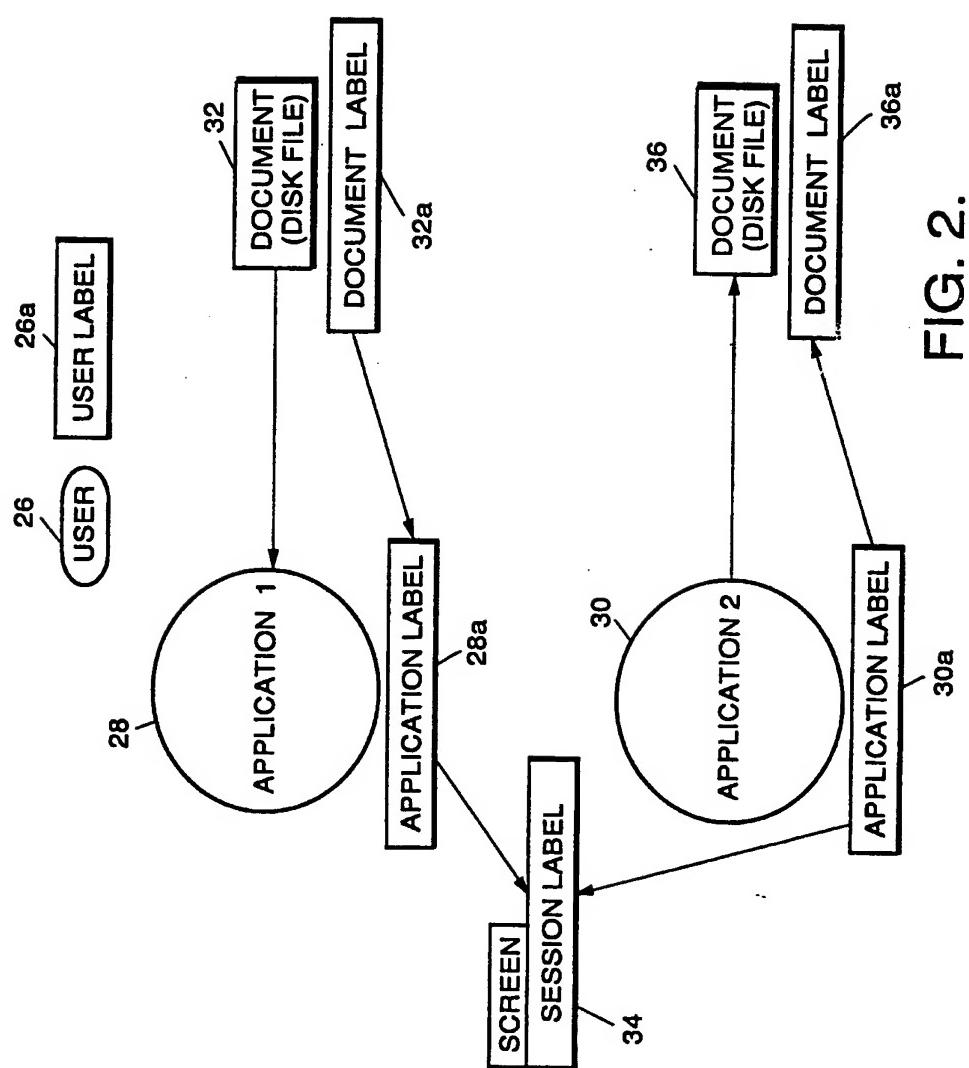
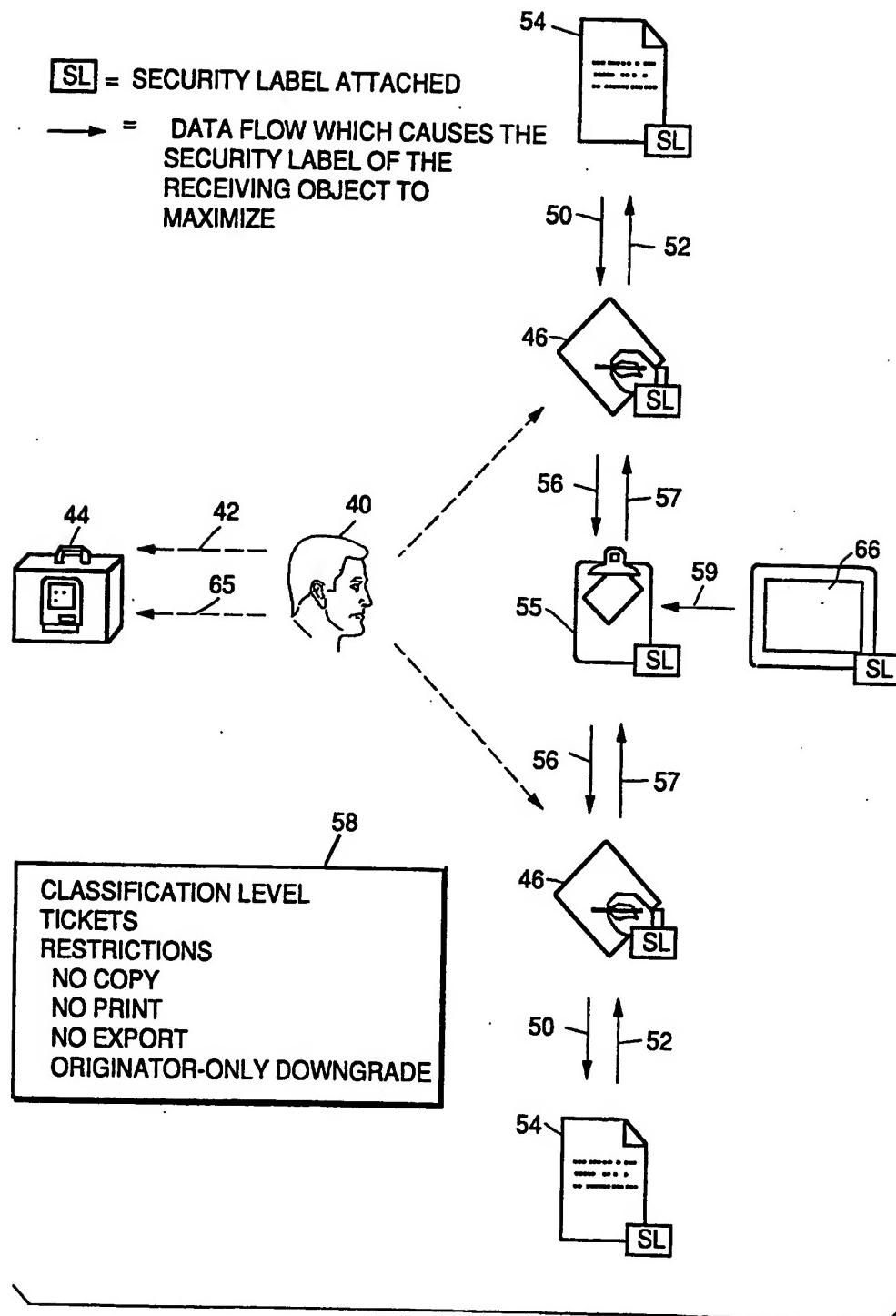


FIG. 2.

3/4

FIG. 3.



4/4

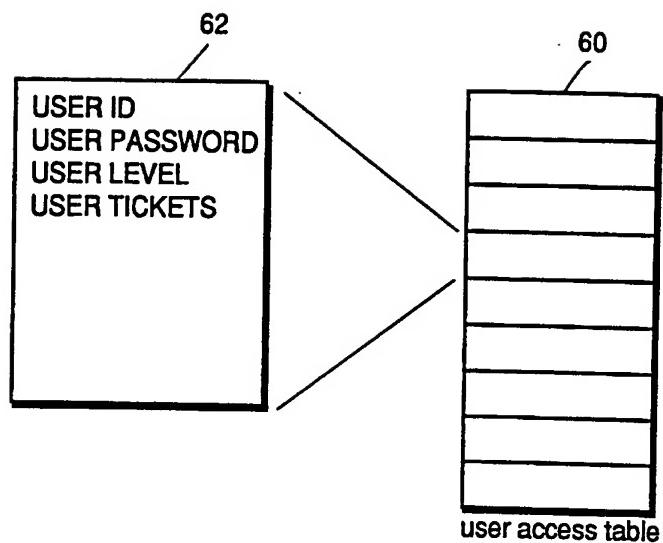


FIG. 4.

**INTERNATIONAL SEARCH REPORT**

International Application No  
PCT/US 94/12457

**A. CLASSIFICATION OF SUBJECT MATTER**  
IPC 6 G06F1/00 G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)  
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US,A,4 956 769 (SMITH) 11 September 1990 see abstract; figures 1,2 see column 1, line 50 - column 6, line 60 -----	I-3,5
Y	-----	4
Y	COMPUTERS & SECURITY, vol.6, no.6, December 1987, AMSTERDAM, NL; pages 479 - 492 M.B.THURAISINGHAM 'Security Checking in Relational Database Management Systems Augmented with Inference Engines' see page 479, right column, line 1 - line 39 see page 483, right column, line 27 - page 484, right column, line 40 -----	4

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

\* Special categories of cited documents :

- 'A' document defining the general state of the art which is not considered to be of particular relevance
- 'B' earlier document but published on or after the international filing date
- 'L' document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- 'O' document referring to an oral disclosure, use, exhibition or other means
- 'P' document published prior to the international filing date but later than the priority date claimed

'T' later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

'X' document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

'Y' document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

'Z' document member of the same patent family

1

Date of the actual completion of the international search

27 February 1995

Date of mailing of the international search report

07.03.95

Name and mailing address of the ISA

European Patent Office, P.B. 5318 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl.  
Fax (+31-70) 340-3016

Authorized officer

Powell, D

## INTERNATIONAL SEARCH REPORT

International Application No  
PCT/US 94/12457

C(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP,A,0 421 409 (IBM) 10 April 1991 see abstract; figures 7-9 see page 7, line 6 - page 8, line 27 see page 9, line 6 - line 25 -----	1-3

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International Application No

PCT/US 94/12457

Patent document cited in search report	Publication date	Patent family member(s)			Publication date
US-A-4956769	11-09-90	NONE			
EP-A-0421409	10-04-91	US-A-	5048085	10-09-91	
		CA-A-	2026739	07-04-91	
		JP-A-	3237551	23-10-91	
		US-A-	5148481	15-09-92	